Evaluation of Collaborative Selfish Node Detection in MANETs and DTNs

Enrique Hernández-Orallo, Manuel D. Serrat Olmos, Juan-Carlos Cano,
Carlos T. Calafate, Pietro Manzoni
Departamento de Informática de Sistemas y Computadores
Universidad Politécnica de Valencia, Valencia, Spain
ehernandez@disca.upv.es, mdserrat@upvnet.upv.es, jucano@disca.upv.es,
calafate@disca.upv.es, pmanzoni@disca.upv.es

ABSTRACT

Mobile ad-hoc Networks (MANETs) and Delay Tolerant Networks (DTN) rely on network cooperation schemes to work properly. Nevertheless, if nodes have a selfish behaviour and are unwilling to cooperate, the overall network performance could be seriously affected. The use of watchdogs is a well-known mechanism to detect selfish nodes. Nevertheless, the detection process performed by watchdogs can fail, generating false positives and false negatives that can induce a wrong behaviour.

In this paper we propose a collaborative watchdog approach based on the diffusion of selfish nodes awareness, that reduces the impact of false positives and false negatives. In order to evaluate the efficiency of our approach, we introduce an analytical model to evaluate the time of detection and the induced overhead of our collaborative watchdog. The results confirm the efficiency of our approach since the detection time of selfish nodes is reduced, the overall overhead is very low, and the impact of false positives and false negatives is minimised.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Wireless communication; I.6 [**Simulation and modelling**]: Model validation and Analysis

Keywords

Wireless network, MANET, DTNs, Selfish Nodes.

1. INTRODUCTION

A Mobile ad-hoc network (MANET) is a network of mobile nodes connected by wireless links without using any pre-existent infrastructure. Nodes are free to move independently in any direction and can directly communicate with each other if a contact occurs (that is, if they are within communication range). Opportunistic and Delay Tolerant Networks (DTNs) constitute an emerging subclass of MANETs where only intermittent connectivity and opportunistic contacts take place. Opportunistic nodes collectively create dynamic networks that are built from short unpredictable contact times as nodes move in and out of connectivity. Applications of such networks include vehicular ad hoc networks (VANETs), and mobile social networks.

In these networks, for a proper functionality, nodes must forward traffic unrelated to their own use. That is, these networks rely on network cooperation schemes to work properly. Nevertheless, in the real world, nodes could have a selfish behaviour, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources (mainly energy).

Several works studied node selfishness in MANETs and DTNs. A first study about misbehaving nodes and how watchdogs can be used to detect them was introduced in [14]. The authors proposed a Watchdog and Pathrater over the DSR protocol to detect non-forwarding nodes, maintaining a rating for every node. In [16] another scheme for detecting selfish nodes based on context aware information was proposed. The CONFINDENT protocol was proposed in [1], which combines a watchdog, reputation systems and bayesian filters from the node and its neighbours to securely detect misbehaving nodes. A Mobile Intrusion Detection System is described in [12] as an advanced watchdog. In [7] an analytical selfish model (which is tied specifically to a routing protocol) is proposed. Recent papers have focused on DTNs. In [11], the author introduces a model for DTN data relaying schemes under the impact of node selfishness. A similar approach is presented in [13] that shows the effect of socially selfish behaviour.

The impact of node selfishness on MANETs has been studied in [18]. When no selfishiness prevention mechanism is installed, the packet delivery rates become seriously degraded, from a rate of 80% when the selfish node ratio is 0, to 30% when the selfish node ratio is 50%. A recent survey [17] shows similar results: the number of packet losses rises 500% when the selfish node ratio increases from 0% to 40%. In DTNs the presence of selfish nodes can seriously degrade the performance of packet transmission. For example, in two-hop relay schemes, if a packet is transmitted to a selfish node the packet is not retransmitted, and so the packet is lost. Thus, if a node knows who are the selfish nodes, it will try to avoid them in order to boost performance.

Therefore, detecting such nodes quickly and accurately

MSWiM'12, October 21–25, 2012, Paphos, Cyprus.

直接评价和间接评价

is essential for the overall network performance. Previous works have demonstrated that watchdogs are appropriate mechanisms to detect misbehaving and selfish nodes. Essentially, watchdog systems overhear wireless traffic and analyse it to decide whether neighbour nodes are behaving in a selfish manner [9]. When the watchdog detects a selfish node it is marked as a *positive* (or a *negative* if it is detected as a non selfish node). Nevertheless, watchdogs can fail on this detection, generating *false positives* and *false negatives* that can seriously degrade the behaviour of the system.

This paper introduces a *collaborative watchdog* approach based on contact dissemination. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network. The goal of our approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives. Although some of the aforementioned papers (such as [1,16]) introduced some degree of collaboration on their watchdog schemes, the diffusion is very costly since they are based on periodic message dissemination.

In order to evaluate the efficiency of our collaborative watchdog we introduce an analytical performance model. Assuming that the occurrence of contacts between two mobile nodes follows a Poisson distribution, we model the network as a Continuous Time Markov chain (CTMC) and derive expressions for obtaining the time and overhead (cost) of detection of selfish nodes. In a preliminary work [6] we introduced a basic collaborative approach based on the diffusion of the positives only. This model is now extended to the distribution of positives and negatives in order to reduce the side effect of false positives and negatives. The problem of false positives and negatives is that they can also be propagated in the network when a collaborative contact occurs, so it is important to reduce this impact. Regarding the false positives and negatives, as far as we know, this is the first work to study their effect on the detection of selfish nodes.

In general, our evaluation shows a significant reduction of the detection time of selfish nodes with a reduced overhead when comparing our collaborative watchdog against a traditional watchdog. From our experiments we conclude that, if only positives are transmitted, the false negatives have little impact on the performance, but the effect of false positives is magnified (due to the sole diffusion of positives). In the other case, if positives and negatives are transmitted, false negatives have a strong impact on performance, and the impact of false positives is reduced. Thus, a mix approach is proposed where the positives are always transmitted, and only a portion of the negatives are transmitted. This way, the effect of false negatives and false positives is minimised, improving the global precision of the watchdog.

2. ARCHITECTURE OVERVIEW

A node's watchdog consists on overhearing the packets transmitted and received by its neighbours in order to detect anomalies, such as the ratio between *packets received* to *packets being retransmitted* [8]. Initially, no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as *positive*, and if it is detected as a non selfish node, it is marked as *negative*. Later on, when this node contacts another node, it *can* transmit this information to it; so, from that moment on, both nodes store information about this positive (or negative). Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly through the collaborative transmission of information that is provided by other nodes.

Figure 1 shows the functional structure of the collaborative watchdog. It has three main components: the watchdog, the diffusion module and the network information:

- The *watchdog* has two functions: the detection of selfish nodes and the detection of new contacts. The detection of selfish nodes can generate the following events about neighbour nodes: `PosEvt` (*positive event*) when the watchdog detects a selfish node, `NegEvt` (*negative event*) when the watchdog believes that a node is not selfish, and `NoInfEvt` (*no info event*) when the watchdog does not have enough information about a node (for example if the contact time is very low or it does not overhear enough messages). The detection of new contacts is based on *neighbourhood* packet overhearing; thus, when the watchdog starts receiving packets from a new node it is assumed to be a new contact, and so it generates an event to the network information module. 邻居节点窃听
- The *diffusion* module has two functions: the transmission and the reception of positives (and negatives). Although positives are always transmitted, sending the negatives can be troublesome, producing excessive messaging or fast diffusion of false negatives. Thus, we introduce a *negative diffusion factor* γ, that is the ratio of negatives that are actually transmitted. This value ranges from 0 (no negatives are transmitted) to 1 (all negatives are transmitted). The significance and importance of the γ factor will be detailed in the evaluation section. Finally, when the diffusion module receives a new contact event from the watchdog, it transmits a message including this information to the new neighbour node. When the neighbour node receives a message, it generates an event to the network information module with the list of these positives (and negatives).
- Network information: A node can have the following internal information about other nodes i: `NoInfo`, `Positive` and `Negative`. `NoInfo` means that it has no information about node i, `Positive` means it believes that node i is selfish and `Negative` means it believes that node i is not selfish. The updating of this information is based on the state transition diagram of figure 2. The network information about the nodes has an expiration time, so after some time without contacts it is deleted.

3. SYSTEM MODEL

The network is modelled as a set of N wireless mobile nodes, with C collaborative nodes and one selfish node ($N = C + 1$). Our goal is to obtain the time and overhead that a set of $D \leq C$ nodes need to detect who is the selfish node in the network. The overhead is the number of information messages transmitted up to the detection time.

First, we are going to characterize the inter-contact times. Then, we model the watchdog and the diffusion modules including the effect of false positives and false negatives.

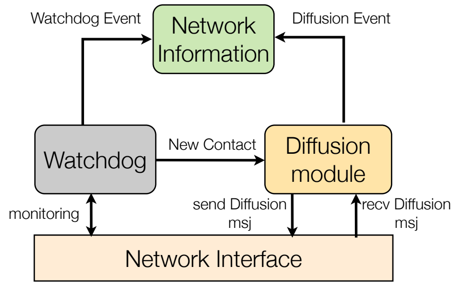


Figure 1: Arquitecture of the collaborative watchdog

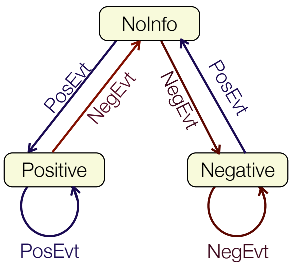


Figure 2: State transition diagram for updating the information about network nodes.

Then, we introduce a model for evaluating the detection of a selfish node, taking into account the effect of false negatives. Since this model evaluates the detection of a selfish positive (that is, a *true* positive), the effect of false positives can not be evaluated through it. Thus, a second model is introduced that evaluates the impact of false positives.

3.1 Characterizing Inter-contact Times

Characterizing inter-contact times (or inter-meeting times) between pairs of nodes is essential for analyzing the performance of contact based protocols. The inter-contact times distribution is obtained by *aggregating* the *individual pair distribution* of all combinations of pairs of nodes in the network. The *individual pair distribution* is defined as the distribution of the time elapsed between two consecutive contacts between the same pair of nodes [15].

The assumption that the aggregated inter-contact time follows an exponential distribution with rate λ has been shown to hold in several mobility scenarios of both human and vehicles [5,13,19]. Empirical results have shown that the aggregated inter-contact time distribution follows a power-law and has a long tail [3], meaning that there are some pairs of nodes that barely experience contact. In [2] it is shown that in a bounded domain (such as the one selected along this paper) the inter-contact distribution is exponential, but in an unbounded domain the distribution is power-law. The dichotomy of this distribution is described in [10]. The work in [4] analyzed some popular mobility traces and found that over 85% of the *individual pair distributions* fit an exponential distribution.

指数分布的合理性

Our performance model assumes an exponential distributed inter-contact rate between nodes and therefore it is suited for both MANETs and DTNs. The main difference is the rate of contact, which is higher in MANETs.

3.2 Modelling system modules

The watchdog is modelled using three parameters: the probability of detection p_d, the ratio of false positives p_{fp}, and the ratio of false negatives p_{fn}. The first parameter, the probability of detection (p_d), reflects the probability that, when a node contacts another node, the watchdog has enough information to generate a `PosEvt` (or `NegEvt`) event. In other words (1-p_d) is the probability of the `NoInfEvt` event. This value depends on the effectiveness of the watchdog, the traffic load, and the mobility pattern of nodes. Furthermore, the watchdog can generate false positives and false negatives. A false positive is when the watchdog generates a positive for a node that is not a selfish node. A false negative is generated when a selfish node is marked as a negative. In order to measure the performance of a watchdog, these values can be expressed as a ratio or probability: p_{fp} is the ratio (or probability) of false positives generated when a node contacts a non-selfish node, and p_{fn} is the ratio (or probability) of false negatives generated when a node contacts a selfish node.

A contact does not always imply collaboration, so we model this probability of collaboration as p_c. The degree of collaboration is a global parameter, and it is used to reflect that either a message with the information about the selfish node is lost, or that a node temporally does not collaborate (for example, due to a failure or simply because it is switched off). In real networks, full collaboration ($p_c = 1$) is almost impossible.

通信故障/切换等引起的信息丢失 => 不能达到全合作状态

Using the previous parameters we can model the probability of the `PosEvt` and `NegEvt` events when a contact occurs:

- `PosEvt` event: there are two possibilities: i) the node contacts with the selfish node and the watchdog detects it, with probability $p_d(1-p_{fn})$; and ii), the node contacts another node that has a `Positive` state about the selfish node with probability p_c. Note that a false positive can also be generated with probability $p_d \cdot p_{fp}$.

- `NegEvt` event: there are two possibilities: i) the node contacts with a non-selfish node with probability $p_d(1-p_{fp})$, and ii) the node contacts another node that has a `Negative`, being the probability $\gamma \cdot p_c$. A false negative can also be generated when it contacts with the selfish node with probability $p_d \cdot p_{fn}$.

bad-mouth；同谋攻击，这里不讨论

Our model assumes that all nodes are selfish or collaborative. Security concerns, such as malicious nodes that spread false information about selfish nodes, are outside the scope of this paper.

3.3 A model for the detection of selfish nodes

In this subsection we introduce an analytical model for evaluating the performance of our collaborative watchdog approach. The goal is to obtain the detection time (and overhead) of a selfish node in a network. This model takes into account the effect of false negatives. False positives do not affect the detection time of the selfish node, so p_{fp} is not introduced in this model. The effect of false positives will be studied in subsection 3.4. For an easier exposition, we first introduce a model for $D = C$, and then this model is extended to the generic case of $D \leq C$.

Using λ we can model the network using a 2D Continuous Time Markov chain (2D-CTMC) with states $(c_p(t), c_n(t))_{t\geq 0}$, where $c_p(t)$ represents the number of collaborative nodes that have a `Positive` state about the selfish node at time t, and $c_n(t)$ represents the number of *collaborative* nodes that have a `Negative` state for the selfish node (note that, in this case, a `Negative` is a false negative). At the beginning all nodes have no information (`NoInfo` state). Then, when a contact occurs, $c_p(t)$ and $c_n(t)$ can be increased by one. As each node can be only in one state, then $c_p(t) + c_n(t) \leq C$. The final (absorbing) state is when $c_p(t) = C$. Our 2D-CTMC model has an initial state $(0, 0)$, a final state $(C, 0)$ and the transient states are all possible permutations that sum C: $\{(0, 1), \ldots (0, C), (1, 0), \ldots (1, C-1), (2, 0) \ldots (2, C-2) \ldots (C-1, 1)\}$. It is easy the derive that the number of permutations that sums C is $\mathrm{P^S}(C) = 0.5(C+1)(C+2)$. We define τ as the number of transient states ($\tau = \mathrm{P^S}(C)$) and υ as the number of absorbing states ($\upsilon = 1$). This model can be expressed using the following transition matrix $\mathbf{P}$ in canonical form:

$$\mathbf{P} = \begin{pmatrix} \mathbf{Q} & \mathbf{R} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} \tag{1}$$

where $\mathbf{I}$ is a $\upsilon \times \upsilon$ identity matrix, $\mathbf{0}$ is a $\upsilon \times \tau$ zero matrix, $\mathbf{Q}$ is a $\tau \times \tau$ matrix with elements p_{ij} denoting the transition rate from transient state s_i to transient state s_j, and $\mathbf{R}$ is a $\tau \times \upsilon$ matrix with elements p_{ij} denoting the transition rate from transient state s_i to the absorbing state s_j.

因为是 连续时间Markov, 所以这里是转移速度

Now, we derive the transition rates p_{ij}. Given the state $s_i = (c_p, c_n)$[1], the following transitions can occur:

- (c_p, c_n) to $(c_p + 1, c_n)$: A new collaborative node has a `Positive` state. The transition probability is $t_P = \lambda(p_d(1-p_{fn}) + p_c c_p)(C - c_p - c_n)$. The term $p_d(1-p_{fn})$ represents the probability of a `PosEvt` event from the watchdog, and $p_c c_p$ the probability of a `PosEvt` event from the diffusion module (it depends on c_p, so this probability is higher if more nodes have a `Positive` state). Finally, the factor $(C - c_p - c_n)$ represents the number of pending collaborative nodes. If there are no pending nodes, this value is 0.

  还没做决定的node的个数

- (c_p, c_n) to $(c_p, c_n + 1)$: A new collaborative node has a `Negative` state (a *false negative*). The transition probability is $t_N = \lambda(p_d p_{fn} + \gamma p_c c_n)(C - c_p - c_n, 0)$.
- (c_p+1, c_n) to (c_p, c_n): A collaborative node that has a `Positive` state changes to `NoInfo`. This occurs when the watchdog or diffusion module generates a `NegEvt` event. So, the transition probability is similar to t_N: $t_{P'} = \lambda(p_d p_{fn} + \gamma p_c c_n)c_p$.
- $(c_p, c_n + 1)$ to (c_p, c_n): A collaborative node that has a `Negative` changes to `NoInfo`. This occurs when the node detect or receives a `PosEvt`. So, the transition probability is similar to t_P: $t_{N'} = \lambda(p_d(1 - p_{fn}) + p_c c_p)c_n$.
- (c_p, c_n) to (c_p, c_n): This is the probability of no changes and is calculated as $t_0 = 1 - t_P - t_N - t_{P'} - t_{N'}$.

For example, for $N = 3$, we have $C = 2$, so $\tau = 5$ and $\upsilon = 1$, the transition matrix is:

$s_i \rightarrow s_j$	0,0	0,1	0,2	1,0	1,1	2,0
0,0	t_0	t_N	0	t_P	0	0
0,1	$t_{N'}$	t_0	t_N	0	t_P	0
0,2	0	$t_{N'}$	t_0	0	0	0
1,0	$t_{P'}$	0	0	t_0	t_N	t_P
1,1	0	$t_{P'}$	0	$t_{N'}$	t_0	0
2,0	0	0	0	0	0	1

[1]For simplicity, we omit the time in the states (that is $(c_p, c_n) = (c_p(t), c_n(t))$)

Using the transition matrix $\mathbf{P}$ we can derive two different expressions: one for the detection time T_d and another for the overall overhead (or cost) O_d. We start with the detection time. From the 2D-CTMC we can obtain how long it will take for the process to be absorbed. Using the fundamental matrix $\mathbf{N} = (\mathbf{I} - \mathbf{Q})^{-1}$, we can obtain a vector $\mathbf{t}$ of the expected time to absorption as $\mathbf{t} = \mathbf{N}\mathbf{v}$, where $\mathbf{v}$ is a column vector of ones ($\mathbf{v} = [1, 1, \ldots, 1]^T$). Each entry t_i of $\mathbf{t}$ represents the expected time to absorption from state s_i. Since we only need the expected time from state $s_1 = (0, 0)$ to absorption (that is, the expected time for all nodes to have a `Positive`), the detection time T_d, is:

到达吸收态的平均时间；

Markov理论中的CK方程解出？；Chapman-Kolmogorov方程

$$T_d = E[T] = \mathbf{v_1}\mathbf{N}\mathbf{v} \tag{2}$$

where T is a random variable denoting the detection time for all nodes and $\mathbf{v_1} = [1, 0, \ldots, 0]$.

Concerning the overhead we need to obtain the number of transmitted messages for each state s_i. First, the duration of each state s_i can be obtained using the fundamental matrix $\mathbf{N}$. By definition, the elements of the first row of $\mathbf{N}$ are the expected times in each state starting from state 0. Then, the duration of state s_i is $f_i = \mathbf{N}(1, i)$.

Now, we calculate the expected number of messages m_i. The number of messages depends on the diffusion model. For an easier exposition, we start with $\gamma = 0$, that is, only the positives are transmitted. From state $s_1 = (0, 0)$ to s_{C+1}=(0,C) no node has a `Positive` state, so no messages are transmitted and $m_1 = 0$. From states $s_{C+2} = (1, 0)$ to $s_{2C+2} = (1, C-1)$, one node has a `Positive` state. In these cases, the `Positive` can be transmitted to all nodes (except itself) for the duration of each state i ($\mathbf{N}(1, i)$) with a rate λ and probability p_c. Then, the expected number of messages can be obtained as $m_i = \mathbf{N}(1, i)\lambda(C - 1)p_c$. From states $s_{2C+3} = (2, 0)$ to $s_{3C+2} = (2, C-2)$, we have two possible senders and $m_i = 2\mathbf{N}(1, i)\lambda(C - 1)p_c$. Summing up, the overhead of transmission (or the expected number of messages) is:

$$O_d = E[M] = \lambda(C - 1)p_c \sum_{i=1}^{\tau} \Phi(s_i)(1, i) \tag{3}$$

where $\Phi(s_i) = c_p$ is the number of nodes with a `Positive` for state s_i. Finally, for $\gamma > 0$, the ratio of nodes c_n that will transmit the negative is precisely γ, so $\Phi(s_i) = c_p + \gamma c_n$.

The previous model can be extended to the case of $D \leq C$. In this generic model the collaborative nodes are divided into two sets: a set with D *detecting* nodes, and a set of $M = C - D$ *middle* (or *non-detecting*) nodes. Note that the *detecting* and *middle* nodes have the same behaviour (both are collaborative nodes). The only purpose of this division is to analytically obtain the time and the overhead required for the subset of *detecting* nodes to detect the selfish node. We therefore use a 4D Continuous Time Markov chain (4D-CTMC) with states $(d_p(t), d_n(t), m_p(t), m_n(t))$, where $m_p(t)$ represents the number of *middle* nodes that have a `Positive`, $m_n(t)$ the *middle* nodes with a `Negative`, d_p the *detecting* nodes with a `Positive` and d_n the *detecting* nodes with a `Negative`. In this case the states must verify the following conditions $d_p(t) + d_n(t) \leq D$ and $m_p(t) + m_n(t) \leq M$. The final (absorbing) states is when $d_p(t) = D$. The number of transient and absorbing states is $\tau = (\mathrm{P^S}(D) - 1)\mathrm{P^S}(M)$ and $\upsilon = \mathrm{P^S}(M)$ respectively. We can derive the transition rates (p_{ij}) of the transition matrix $\mathbf{P}$ in a way that is similar to the previous model:

$$p_{ij} = \begin{cases} \lambda(p_d(1-p_{fn}) + p_c(m_p+d_p)) \cdot \mathcal{M}() & m_p+ \\ \lambda(p_d p_{fn} + \gamma p_c(m_n+d_n)) \cdot \mathcal{M}() & m_n+ \\ \lambda(p_d p_{fn} + \gamma p_c(m_n+d_n)) \cdot m_p & m_p- \\ \lambda(p_d(1-p_{fn}) + p_c(m_p+d_p)) \cdot m_n & m_n- \\ \lambda(p_d(1-p_{fn}) + p_c(m_p+d_p)) \cdot \mathcal{D}() & d_p+ \\ \lambda(p_d p_{fn} + \gamma p_c(m_n+d_n)) \cdot \mathcal{D}() & d_n+ \\ \lambda(p_d p_{fn} + \gamma p_c(m_n+d_n)) \cdot d_p & d_p- \\ \lambda(p_d(1-p_{fn}) + p_c(m_p+d_p)) \cdot d_n & d_n- \end{cases} \quad (4)$$

where $\mathcal{M}() = (M - m_p - m_n$, $\mathcal{D}() = D - d_p - d_n$, $x+$ represents a transition from state $(\cdots, x, \cdots)$ to $(\cdots, x+1, \cdots)$, and $x-$ represents a transition from state $(\cdots, x+1, \cdots)$ to $(\cdots, x, \cdots)$. Finally, p_{ii} is $1 - \sum_{j \neq i} p_{ij}$

Using transition matrix $\mathbf{P}$ we can obtain the detection time using equation 2 and the overhead from equation 3, where $\Phi(s_i) = d_p + m_p + \gamma(d_n + m_n)$.

3.4 A model for false positives

In this subsection we develop a model for evaluating the effect of the false positives. When a node has a false positive the problem is that, due to the diffusion of positives, this false positive can be quickly distributed in the network. A way to evaluate this diffusion is to obtain the time (and cost) that a set of D nodes have a false positive about a given node. Following the same process that in the model for the false negatives, we have (for $D = C$) a 2D-CMTC with the same states (c_p, c_n), but in this case c_p represents the number of nodes with false positives, and c_n the number of nodes with a negative. The transition rates (p_{ij}) of the transition matrix $\mathbf{P}$ are:

$$p_{ij} = \begin{cases} \lambda(p_d p_{fp} + p_c c_p) \cdot \mathcal{C}() & c_p+ \\ \lambda(p_d(1-p_{fp}) + \gamma p_c c_n) \cdot \mathcal{C}() & c_n+ \\ \lambda(p_d(1-p_{fp}) + \gamma p_c c_n) \cdot c_p & c_p- \\ \lambda(p_d p_{fp} + p_c c_p) \cdot c_n & c_n- \end{cases} \quad (5)$$

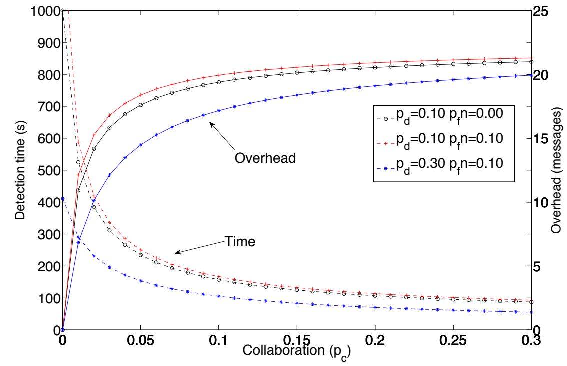
where $\mathcal{C}() = C - c_p - c_n$. We can see that the transition rates are the same than in the false negative model if we replace $p_{fp} = 1 - p_{fn}$. Therefore, we can use the previous model for obtaining the detection time T_d and the overhead O_d.

4. EVALUATION

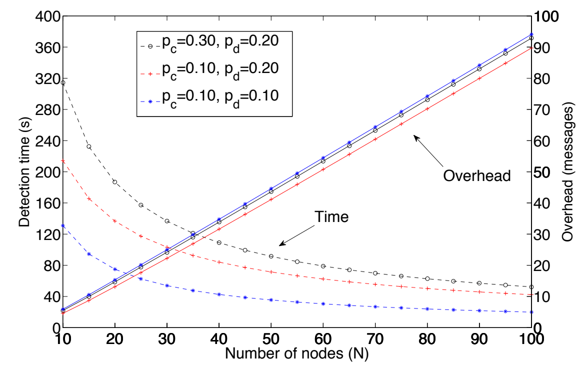
This section is devoted to evaluating the performance of our collaborative watchdog approach. First, we study the global performance depending on the degree of collaboration and the number of nodes. Then, we focus our study on the impact of false negatives and false positives. Finally, we compare our approach to the classic periodic diffusion model. Note that, since λ is a multiplying factor of the transition matrix $\mathbf{P}$, the concluding results of this section are valid for any value of λ. Thus, for the evaluations that follows, we consider a λ value of 0.01 contacts/s, which has been shown to be a valid value in vehicular scenarios [19].

4.1 Impact of collaboration and nodes

The first evaluation shows the impact that the degree of collaboration (p_c) has over the efficiency of the collaborative watchdog for $\gamma = 0$ (that is, only positives are transmitted). Figure 3a shows the detection time and overhead for one detecting node $(D = 1)$ in a network with 25 nodes $(N = 25)$ with different probabilities of detection and false negatives



(a)



(b)

Figure 3: Impact of collaboration and nodes for only positives diffusion $(\gamma = 0)$. a) depending on collaboration in a network of $N = 25$, b) depending on the number of nodes.

(p_d, p_{fn}). We observe that when increasing the degree of collaboration from 0 to 0.2 the detection time is reduced exponentially. The effect of p_d is the expected: for greater values of p_d, the detection time is reduced. The effect of false negatives produces a small increase on the detection time when p_{fn} increases, but this will be studied later.

When repeating the previous experiment to evaluate the detection time (and overhead) required by all nodes to detect the selfish node (that is, $D = N - 1 = 24$) we obtained a similar pattern. For example, for $p_d = 0.1$ and $p_{fn} = 0.1$, the detection time with no collaboration $(p_c = 0)$ is $12,993s$. This value can be greatly reduced by using our collaborative watchdog. Thus, if all nodes implement the collaborative approach, and even for a low collaboration rate $(p_c = 0.2)$, the detection time for all nodes is reduced to $191s$ with an overhead of just 85 messages.

We now evaluate the impact of the number of nodes, ranging from 10 to 100 (see figure 3b). Three different sets of values for p_c and p_d were used. In all the cases the value of p_{fn} is 0.1. We observe that, in general, the greater the number of nodes, the smaller the detection time and the greater the number of messages. The main reason is that, when the number of nodes is greater, the number of contacts is increased and so the information about the positive detection is disseminated more quickly. Reduced values for the collaboration and detection probabilities imply greater detection

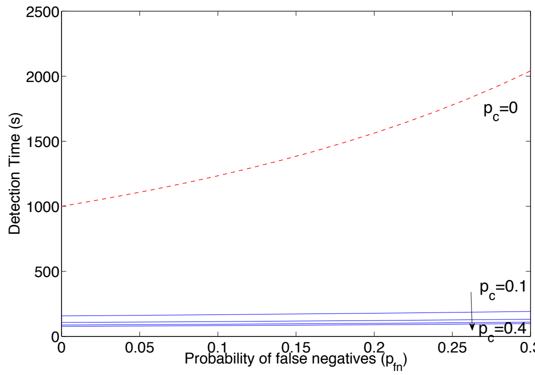


Figure 4: Evaluation of the impact of false negatives for $p_d = 0.1$ with $\gamma = 0$ for several values of p_c

times (as expected). Nevertheless, the cost depends mainly on N.

4.2 Impact of false negatives

The goal of the following experiments is to evaluate the impact of false negatives. Figure 4 shows the detection time for one node ($D = 1$) in a network of 25 nodes ($N = 25$) depending on false negatives for several values of p_c We can see that the detection time is greatly reduced when p_c is greater than zero, and that false negatives do not affect this detection time. Regarding the overhead, the experiment showed little influence on the number of messages, that is always around 20 messages. The results show that false negatives have a small influence on the detection time.

Figure 5 shows the results for $\gamma = 1$ (that is, full transmission of the negatives) with the same network parameters ($N = 25$, $S = 1$, $D = 1$). The results when p_{fn} is zero are very similar to the only positives diffusion case ($\gamma = 0$). However, when p_{fn} is not zero we can observe that for low degrees of collaboration the detection time decreases and the overhead increases in a similar way to the only positives case. Nevertheless, when p_c increases, the detection time increases again, and the overhead increases exponentially. It seems that the collaboration amplifies the impact of false negatives. This effect is confirmed in figure 6, where we can see that the curves for greater values of p_c have a greater exponential slope. This is particularly evident in the ($p_d = 0.1$,$p_{fn} = 0.1$) curve. Regarding the overhead, the results showed a similar behaviour (in general, a greater detection time implies a greater overhead).

Summing up, if only positives are transmitted, the detection time is greatly reduced and the impact of false negatives is also reduced; however, when all known negatives are transmitted, collaboration amplifies the effect of false negatives.

4.3 Impact of false positives

In this subsection we evaluate the influence of false positives using the model developed in section 3.4. In this case, we expect that the diffusion of negatives reduces the influence of false positives and that when γ is zero, the influence of false positives will be amplified. Figure 7a shows the detection time for $\gamma = 0$. We observe that for the curves where $p_c > 0$ the effect of false positives is amplified, leading to a drastic reduction on the detection time, meaning that these false positives are spread on the network rather quickly. For

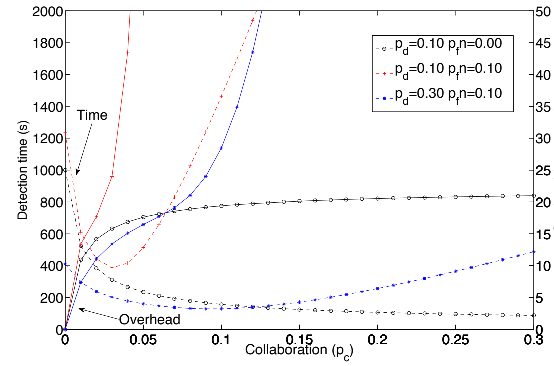


Figure 5: Detection time and overhead depending on collaboration for full transmission of negatives ($\gamma = 1$).

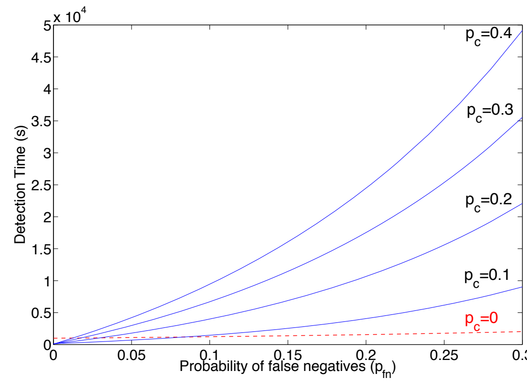
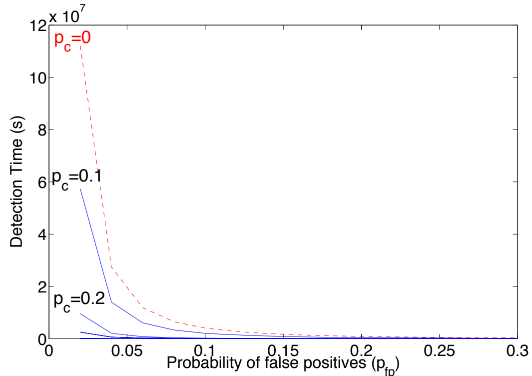


Figure 6: Evaluation of the impact of false negatives with $\gamma = 1$ for several values of p_c

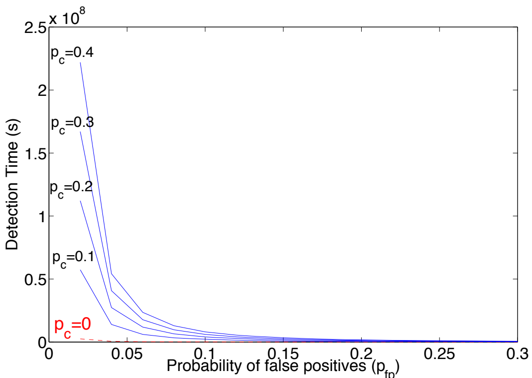
example, for $p_{fp} = 0.1$, the detection time is $1 \times 10^5 s$ for $p_c = 0$ and $1394s$ for $p_c = 0.1$. This detection time is equivalent to a value of $p_{fp} = 0.82$ when there is no collaboration ($p_c = 0$). Thus, the undesired effect is that the false positives rate is increased. Consequently, we need to transmit the negatives in order to compensate for these false positives. Figure 7b shows the results for $\gamma = 1$. In this case, we can see that the detection time is highly increased when the collaboration increases and so the effect of false positives is reduced.

Therefore, we have the inverse effect that in the false negatives case. If only positives are transmitted the effect of false positives is magnified and so the transmission of negatives is necessary in order to reduce the impact of false positives. This effect can be regulated using the γ factor. We evaluated the same scenario selected in figures 6 and 7a for $\gamma = 0.25$. First, we can see in figure 8a that the detection time is reduced, even if the ratio of false negatives is high. Second, figure 8b shows that the detection time is increased when the collaboration increases, effectively reducing the effect of false positives. For example, for $p_{fp} = 0.1$, the equivalent false positive rate for collaboration of $p_c = 0.3$ is reduced to 0.05.

The conclusions is that the γ value must be tuned up in order to achieve the desired behaviour. A γ value near to zero greatly reduces the detection time of selfish nodes, but increases the diffusion of false positives. A value near to one

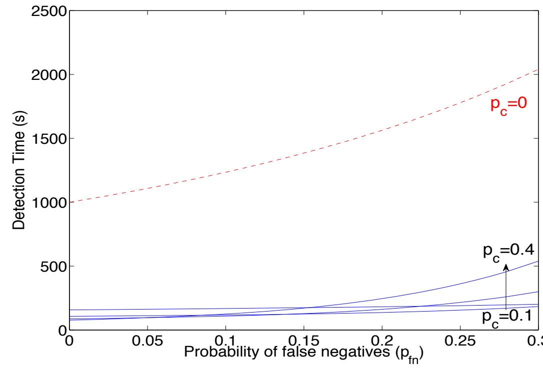


(a)

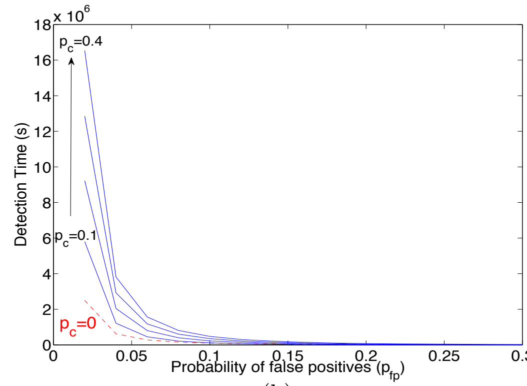


(b)

Figure 7: Evaluation of the impact of false positives a) when $\gamma = 0$, b) when $\gamma = 1$.



(a)



(b)

Figure 8: Results for a controlled diffusion of negatives $\gamma = 0.25$ a) impact of false negatives, b) impact of false positives.

increases the detection time (due to the the effect of the false negatives), but reduces the diffusion of false positives.

4.4 Comparison with other approaches

We now proceed by comparing our collaborative watchdog approach with previous cooperative approaches that use periodic messages for the diffusion of information about selfish node detections (such as the ones presented in [1,16]). Note that this comparison focuses only on the diffusion protocol. If a node has information about a positive (or negative), it will periodically broadcast a message with a given period P. This message will be received by all nodes that are within the communication range of the sender. The performance of this protocol clearly depends on the period P. A short period will reduce the detection time, but the number of messages transmitted (the overhead) will be high. A large period will increase the detection time by reducing the overhead.

The comparison of both protocols was based on simulations. We implemented the periodic diffusion protocol, as described in the previous paragraph. In this periodic approach only the positives are sent. Regarding our collaborative approach, the watchdog parameters are ($p_{fp} = 0.17$, $p_{fn} = 0.08$,$p_d = 0.11$), that were obtained based on a set of real test bed experiments from [9]. The rest of parameters are $p_c = 0.2$ and $\gamma = 0.25$. By using the ns-2 *setdest* command we generate mobility scenarios that are used to simulate both approaches.

Figure 9 shows the detection time and overhead for the periodic diffusion protocol when the its period P ranges from 1 to 30s with three different number of nodes ($N = 30, 40, 50$). The results confirm that increasing the period P implies a higher detection time while the overhead is reduced. We compare these results with the detection time and overhead values for our collaborative watchdog (that are in the legend of the plot for each value of N). For example, for $N = 50$, the periodic diffusion for periods below 4s has a shorter detection time than our model, but with a higher overhead. For example, for $P = 2s$, the detection time is 963s (a reduction of 9%) and the overhead is 5212 messages (an increment of 4738%) with respect to our collaborative watchdog approach. For $P = 4s$, the detection time is similar to our approach, and the overhead is 3210 messages (2972% higher). Regarding the false positives, in the periodic model the diffusion time of false positives is reduced for low values of P. For example, for $N = 40$ the detection time of false positives is reduced from $15,024s$ when there is no diffusion of positives to $900s$ when $P = 1$. This is equivalent to a false positives rate of 0.72, that is an unreasonable value.

Summing up, although using periodic diffusion can reduce the detection time slightly, this implies a large overhead and the impact of false positives is very high, so is not a viable strategy for low period values.

5. CONCLUSIONS

This paper proposes a *collaborative watchdog* to improve the detection time and efficiency of selfish nodes, reducing the effect of false positives of negatives (that is, improving the global precision of the detection process). The col-

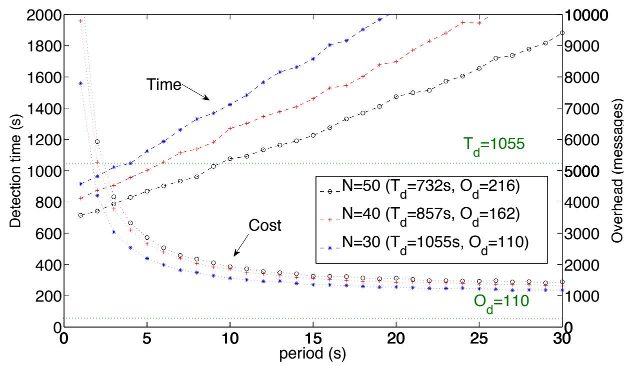


Figure 9: Detection time and overhead depending on period P for the periodic approach. The main parameters for the mobility model are mean-speed = 5m/s, side-area = 1000 m, pause-interval = 1s, range = 100m

laborative watchdog is based on the diffusion of the known positives and negatives. When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positives (and negatives).

Numerical results show that our collaborative watchdog can reduce the overall detection time with respect to the original detection time with no collaboration scheme with a reduced overhead (message cost). This reduction is very significant, with a percentage of reduction ranging from 20% for very low degree of collaboration to 99% for higher degrees of collaboration. Regarding the overall precision we show how by selecting a factor for the diffusion of negatives the harmful impact of both false negative and false positive is diminished. Summing up, the controlled effect of collaboration of our approach can reduce the detection time while increasing the global accuracy using a moderate local precision watchdog.

As future work, we plan to extend the model to introduce a reputation scheme in order to give more or less weight to the information received from other nodes.

6. ACKNOWLEDGMENTS

This work was partially supported by the *Ministerio de Ciencia e Innovación*, Spain, under Grant TIN2011-27543-C03-01.

7. REFERENCES

[1] S. Buchegger and J.-Y. Le Boudee. Self-policing mobile ad hoc networks by reputation systems. *Communications Magazine, IEEE*, 43(7):101 – 107, jul. 2005.

[2] H. Cai and D. Y. Eun. Crossing over the bounded domain: From exponential to power-law intermeeting time in mobile ad hoc networks. *Networking, IEEE/ACM Transactions on*, 17(5):1578 –1591, oct. 2009.

[3] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott. Impact of human mobility on opportunistic forwarding algorithms. *IEEE Transactions on Mobile Computing*, 6:606–620, Jun 2007.

[4] W. Gao, Q. Li, B. Zhao, and G. Cao. Multicasting in delay tolerant networks: a social network perspective. In *Proceedings of MobiHoc '09*, pages 299–308, 2009.

[5] R. Groenevelt, P. Nain, and G. Koole. The message delay in mobile ad hoc networks. *Performance Evaluation*, 62:210–228, October 2005.

[6] E. Hernández-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni. Improving selfish node detection in manets using a collaborative watchdog. *IEEE Communications Letters*, 16(5):642–645, 2012.

[7] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz. On the effect of node misbehavior in ad hoc networks. In *Proceedings of IEEE International Conference on Communications, ICC'04*, pages 3759–3763, 2004.

[8] J. Hortelano, J.-C. Cano, C. T. Calafate, M. de Leoni, P. Manzoni, and M. Mecella. Black hole attacks in p2p mobile networks discovered through bayesian filters. In *In P2P Collaborative Distributed Virtual Environments (P2P CDVE 2010)*, 2010.

[9] J. Hortelano, J. C. Ruiz, and P. Manzoni. Evaluating the uselfusness of watchdogs for intrusion detection in vanets. In *In ICC'10 Workshop on Vehicular Networking and Applications*, 2010.

[10] T. Karagiannis, J.-Y. Le Boudec, and M. Vojnović. Power law and exponential decay of inter contact times between mobile devices. In *Proceedings of MobiCom '07*, pages 183–194. ACM, 2007.

[11] M. Karaliopoulos. Assessing the vulnerability of dtn data relaying schemes to node selfishness. *Communications Letters, IEEE*, 13(12):923 –925, december 2009.

[12] F. Kargl, A. Klenk, S. Schlott, and M. Weber. Advanced detection of selfish or malicious nodes in ad hoc networks. In *In Proceedings of the 1st European on Security in Ad-Hoc and Sensor Networks*, pages 152–165. Springer Verlag, 2004.

[13] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng. The impact of node selfishness on multicasting in delay tolerant networks. *Vehicular Technology, IEEE Transactions on*, 60(5):2224 –2238, jun 2011.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of MobiCom '00*, pages 255–265, 2000.

[15] A. Passarella and M. Conti. Characterising aggregate inter-contact times in heterogeneous opportunistic networks. In *Proceedings of the 10th international conference on Networking*, pages 301–313, 2011.

[16] K. Paul and D. Westhoff. Context aware detection of selfish nodes in dsr based ad-hoc networks. In *In Proceedings of IEEE Globecom*, 2002.

[17] C. Toh, D. Kim, S. Oh, and H. Yoo. The controversy of selfish nodes in ad hoc networks. In *Proceeding of Advanced Communication Technology (ICACT), 2010*, volume 2, pages 1087 –1092, feb. 2010.

[18] Y. Yoo, S. Ahn, and D. Agrawal. A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks. In *Proceedings of IEEE ICC*, volume 5, pages 3005 – 3009 Vol. 5, may 2005.

[19] H. Zhu, L. Fu, G. Xue, Y. Zhu, M. Li, and L. M. Ni. Recognizing exponential inter-contact time in vanets. In *Proceedings of INFOCOM'10*, pages 101–105, 2010.